

UNITS IN METABELIAN GROUP RINGS: NON-SPLITTING EXAMPLES FOR NORMALIZED UNITS

Klaus W. ROGGENKAMP

Mathematics Institut B, Universität Stuttgart, West Germany

Leonard L. SCOTT

Department of Mathematics, University of Virginia, Charlottesville, VA 22903, USA

Communicated by H. Bass

Received 1 May 1982

Revised 1 June 1982

Let G be a finite group and $V(G)$ the normalized units in the integral group ring $\mathbb{Z}G$. That is an element of $V(G)$ is a unit in $\mathbb{Z}G$ which maps to 1 under the augmentation map $\mathbb{Z}G \rightarrow \mathbb{Z}$. The question has been raised by Dennis [4] as to when the natural inclusion $G \rightarrow V(G)$ is split. Perhaps the main interest in this question is that the group ring problem is answered very instructively, whenever a splitting exists which can be achieved with a map $V(G) \rightarrow G$ whose kernel is torsion free.

We give here the first examples which show that the map $G \rightarrow V(G)$ does not always split.

We note the following ring-theoretic consequence: Since there exists a splitting $\varphi: V(G) \rightarrow G$ if and only if there exists a ring \mathfrak{R} such that G has a normal complement in the units in \mathfrak{R} , our examples show that there are groups which can not be split subgroups of the unit group in *any* ring.

This area of units in group rings has been of considerably activity recently [10], [9], [1], [12] and [3]. The most far reaching result is that of Cliff-Sehgal-Weiss:

Theorem. *If G has an abelian normal subgroup H with G/H abelian of odd order, then there is a splitting, and it can be achieved by a map $V(G) \rightarrow G$ whose kernel is torsion free.*

So the open metabelian cases are groups G which do not have an abelian normal subgroup H with G/H abelian of odd order. Let G be metabelian with an abelian normal subgroup H such that G/H is abelian of even order. We then write $G/H = A_0 \times A_1$, A_0 a 2-group and A_1 of odd order. Since a possible failure of splitting seems to come from the 2-part of G/H , we shall consider the following two cases. (C_n stands for the cyclic group of order n .)

Case (i): $A_1 = 1$. Then C_8 must be a subgroup of A_0 , in order that $V(A_0)$ has non-trivial units – this is necessary for failure of splitting. We shall show that the Frobenius group

$$G = C_{73} \rtimes C_8$$

does not allow a splitting of the natural inclusion $G \rightarrow V(G)$.

Case (ii): $V(A_0)$ has only trivial units; i.e. the exponent of A_0 is at most 4. In this case we consider metacyclic Frobenius groups $C_p \rtimes (A_0 \times A_1)$, where p is a prime and $|A_0| \leq 4$. Then both $V(C_p \rtimes A_0)$ and $V(C_p \rtimes A_1)$ allow a splitting as above. However, we shall show that

$$G = C_{241} \rtimes C_{10}$$

does not allow a splitting of the natural inclusion $G \rightarrow V(G)$.

These examples indicate that the theorem of Cliff–Sehgal–Weiss is – as a general statement – best possible. However, we would like to point out a positive result, which indicates that a necessary and sufficient condition for a splitting of units of metabelian groups is not so easily obtained.

Proposition 1. *Let $G = C_p \rtimes C_{p-1}$ be an affine Frobenius group. Then there exists a splitting $\varphi: V(G) \rightarrow G$ with $\text{Ker } \varphi$ torsion free.*

This was also observed by Sekiguchi [14].

The above proposition is part of the following more general phenomenon: Let G be metabelian with abelian normal subgroup H and abelian quotient $G/H =: B$. Then the conjugation action of B on H induces a homomorphism

$$\mu: B \rightarrow \text{Aut}(H).$$

Assume that μ is surjective, then there is a splitting $\varphi: V(G) \rightarrow G$ with $\text{Ker } \varphi$ torsion free.

Let us turn to metacyclic Frobenius groups of the form $G_0 = C_p \rtimes C_m$, p a prime. In case $m = p - 1$, G_0 obviously satisfies the hypothesis of Proposition 1. Hence there exists a splitting

$$\varphi_0: V(G_0) \rightarrow G_0.$$

Let now $G = C_{73} \rtimes C_8$ or $G = C_{241} \rtimes C_{10}$ and $G_0 = C_{73} \rtimes C_{72}$ or $G_0 = C_{241} \rtimes C_{240}$. Then $G \leq G_0$ and

$$\text{Im } \varphi_0|_{V(G)} \not\supseteq G,$$

because, if $\text{Im } \varphi_0|_{V(G)} \subset G$, then $\varphi|_{V(G)}$ would be a splitting; but no such splitting exists.

This note is organized as follows: In Section 1 we prove the proposition and consider splittings ‘which come from ideals’, a concept also used in [3]. Using this we show that for our groups $C_{73} \wr C_8$ and $C_{241} \wr C_{10}$, a splitting can not come from an ideal. In Section 2 we use the congruence subgroup theorem of Bass–Milnor–Serre [2] to show that every splitting must essentially come from an ideal. Most of our results should hold for metabelian groups in general; however, we did not elaborate on this, since we are interested in particular metacyclic groups.

Erratum: The first author wants to point out a mistake in [11] where he claimed that metacyclic Frobenius groups always allow a splitting. The point is that the sequences \mathfrak{E}_1 and \mathfrak{E}_2 [11, p. 264] are not equivalent. The mistake was also noted by S.K. Sehgal.

We remark that in the proof of the theorem of Cliff–Sehgal–Weiss [3] one of the main difficulties is to prove that $V(G) \rightarrow G$ has a torsion-free kernel. This was essentially proved in Jackson’s thesis of 1968 [7] and brought up to date in [12]. According to a letter of Sekiguchi [14], Miyata has done the same.

1. Splitting by ideals

Throughout $G = H \wr C$ is a metacyclic Frobenius group,

$$\begin{aligned} H &= \langle h_0 : h_0^p = 1 \rangle, \quad p \geq 7, \quad p \text{ a prime,} \\ C &= \langle c : c^m = 1 \rangle, \quad m > 2, \quad m \mid (p-1). \end{aligned} \quad (1)$$

The split exact sequence

$$\mathfrak{E}: 1 \rightarrow H \rightarrow G \rightarrow C \rightarrow 1$$

gives rise to the split exact sequence of normalized units

$$\mathfrak{E}_V: 1 \rightarrow V_H(G) \rightarrow V(G) \rightarrow V(C) \rightarrow 1, \quad (*)$$

where

$$V_H(G) = \{1 + x : x \in \eta \uparrow^G\} \cap V(G),$$

and $\eta \uparrow^G = \eta \mathbb{Z}H \approx \eta \otimes_{\mathbb{Z}H} \mathbb{Z}G$, η being the augmentation ideal $\mathbb{Z}H$.

We first recall some results on the structure of $\mathbb{Z}G$ – for the details we refer to [5], [6], [13]. (These results can also be proved by computing the index of $\mathbb{Z}G$ in a maximal order, as was done by H. Jacobinski (unpublished).)

Let $e_0 = 1 - |H|^{-1} \sum_{h \in H} h$, then e_0 is a central primitive idempotent in $\mathbb{Q}G$ and

$$\mathbb{Z}Ge_0 = \begin{pmatrix} R & \cdots & R \\ \mathfrak{p} & \ddots & \vdots \\ \vdots & \ddots & \mathfrak{p} \\ \mathfrak{p} & \cdots & \mathfrak{p} & R \end{pmatrix}_m,$$

where $R = \text{Fix}_C \mathbb{Z}[\sqrt[m]{1}]$, by viewing C as a subgroup of $\text{Gal}(\mathbb{Q}(\sqrt[m]{1})/\mathbb{Q})$, and \mathfrak{p} is the

unique maximal ideal in R above p , with $R/p = \mathbb{F}_p$ the field with p elements.

In particular, the natural representation of G in $\mathbb{Z}Ge_0$ has the form

$$v(g) = \begin{pmatrix} v_1(g) & \cdots & & \\ \vdots & v_2(g) & * & \vdots \\ & ** & \ddots & \\ & \cdots & & v_m(g) \end{pmatrix}_m \quad (2)$$

where the elements in $*$ lie in R and those in $**$ lie in p .

Moreover, easy computations show

$$\eta \uparrow^G = \begin{pmatrix} p & R & \cdots & R \\ \vdots & & \ddots & \\ p & \cdots & p \end{pmatrix}_m; \quad \eta^2 \uparrow^G = \begin{pmatrix} p & p & R & \cdots & R \\ \vdots & & \ddots & & \\ p & & & & p \\ p^2 & p & \cdots & & p \end{pmatrix}_m. \quad (3)$$

and so

$$\eta \uparrow^G / \eta^2 \uparrow^G = \begin{pmatrix} \mathbb{F}_p & & \\ & \ddots & \\ & & \mathbb{F}_p \\ p & & & \end{pmatrix}_m, \quad \bar{p} = p/p^2.$$

Let I be a two-sided $\mathbb{Z}G$ -ideal contained in $\eta \uparrow^G$. Then we put

$$V_I(G) = \{1 + y : y \in I\} \cap V(G), \quad (4a)$$

so that

$$V_H(G) = V_{\eta \uparrow^G}(G). \quad (4b)$$

Claim 1. (i) *We have a natural isomorphism*

$$\sigma : \eta \uparrow^G / \eta^2 \uparrow^G \simeq V_H(G) / V_{\eta^2 \uparrow^G}(G),$$

which is equivariant with respect to the conjugation action of $V(G)$.

(ii) *The composition factors of $\eta \uparrow^G / \eta^2 \uparrow^G$ under C -conjugation are isomorphic to H with C -conjugation.*

(iii) $v_i v_{i+1}^{-1} |_C$ modulo p is the conjugation representation of C on $H = \mathbb{F}_p$, $1 \leq i \leq n$, $n+1=1$.

Proof. (i) We define

$$\sigma^{-1} : V_H(G) / V_{\eta^2 \uparrow^G}(G) \rightarrow \eta \uparrow^G / \eta^2 \uparrow^G$$

by

$$(1+x)V_{\eta^2 \uparrow^G}(G) \mapsto x + \eta^2 \uparrow^G.$$

Then σ^{-1} is well defined by (4), and it is a group homomorphism since

$$(1+x)(1+y) = (1+x+y) + xy \quad \text{and} \quad xy \in \eta^2 \uparrow^G.$$

Moreover, it is injective by the construction of $V_{\eta^2 \uparrow G}(G)$, and σ^{-1} surely is equivariant with respect to conjugation by $V(G)$.

By [5, 3.5], $V_I(G) = \{1 + x, x \in I, \det 1 + x \in R^*\}$, where R^* denotes the units in R . Hence

$$|V_H(G)/V_{\eta^2 \uparrow G}(G)| = p^m = |\eta \uparrow^G / \eta^2 \uparrow^G|.$$

Thus σ^{-1} is an isomorphism.

(ii) As C -module under conjugation we have

$$\eta \uparrow^G / \eta^2 \uparrow^G = \bigoplus_{i=0}^m \{(h-1)c^i\}_{h \in H},$$

and so all composition factors of $\eta \uparrow^G / \eta^2 \uparrow^G$ are isomorphic to H as C -modules via conjugation.

(iii) We now compute the action using the representation v . If an element of $\eta \uparrow^G / \eta^2 \uparrow^G$ is represented by

$$x = \begin{pmatrix} 0 & a_1 & 0 & \cdots & 0 \\ \vdots & \ddots & a_2 & & \vdots \\ & & & \ddots & 0 \\ 0 & & & & \ddots & a_{m-1} \\ a_m & 0 & \cdots & & & 0 \end{pmatrix},$$

then an easy computation shows

$$v(c)xv(c^{-1}) = \begin{pmatrix} 0 & & v_1(c)v_2(c^{-1})a_1 & 0 & \cdots & 0 \\ 0 & \ddots & & \ddots & & \vdots \\ \vdots & & \ddots & & \ddots & 0 \\ 0 & & & \ddots & & 0 \\ v_m(c)v_1(c^{-1})a_m & 0 & \cdots & 0 & v_{m-1}(c)v_m(c^{-1})a_{m-1} & \end{pmatrix}.$$

Since v is a representation, we have $v_i(c^{-1}) = v_i(c)^{-1}$, and by (ii) all C -composition factors of $\eta \uparrow^G / \eta^2 \uparrow^G$ are isomorphic to H as C -module, so the statement follows. \square

We now turn to *splittings which come from ideals*. All the previous splittings – including [3] – were constructed in the following way: Look at the two-sided $\mathbb{Z}G$ -ideals I with $\eta \uparrow^G \subset I \subset \eta \uparrow^G$ and $\eta \uparrow^G / I \cong H$ as abelian groups. Then by Claim 1, $V_I(G)$ is a normal subgroup of $V(G)$, and $V_H(G)/V_I(G) \cong H$ as abelian groups. The sequence $\mathfrak{G}_V(*)$ gives rise to the exact sequence

$$\mathfrak{G}_V: 1 \rightarrow V_H(G)/V_I(G) \rightarrow V(G)/V_I(G) \rightarrow V(C) \rightarrow 1.$$

Since $V_H(G)/V_I(G) \cong_{\text{nat}} \eta \uparrow^G / \eta^2 \uparrow^G$ is abelian, $V(C)$ acts on $V_H(G)/V_I(G)$ by conjugation. This conjugation is induced from the conjugation of $V(G)$ on $V_H(G)$; hence

the canonical map

$$\varphi': V_H(G) \rightarrow V_H(G)/V_I(G)$$

is $V(G)$ -equivariant. The action of $V(C)$ on $V_H(G)/V_I(G) \cong H$ leads to a group homomorphism

$$\mu_I: V(C) \rightarrow \text{Aut}(H). \quad (5)$$

On the other hand, C acts on H by conjugation, and so we have a homomorphism

$$\mu: C \rightarrow \text{Aut}(H).$$

Claim 2. *Let I be as above, and assume $\text{Im } \mu_I \subset \text{Im } \mu$, then there is a splitting for the natural injection $G \rightarrow V(G)$.*

Proof. By Higman's theorem [6],

$$V(C) \cong C \times T,$$

where T is free abelian of finite rank. Since $\text{Im } \mu_I \subset \text{Im } \mu \cong C$ we can choose the complement T in such a way that

$$T \subset \text{Ker } \mu_I.$$

Let now

$$\varphi: V(C) \rightarrow C$$

be the projection with $\text{Ker } \varphi = T$. We then form the pullback along φ :

$$\begin{array}{ccccccc} \mathfrak{E}: & 1 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & C & \longrightarrow & 1 \\ & & & \parallel & & \uparrow & & \uparrow \varphi & & \\ \mathfrak{E}_\varphi: & 1 & \longrightarrow & H & \longrightarrow & X & \longrightarrow & V(C) & \longrightarrow & 1 \end{array}$$

Then \mathfrak{E}_φ is split exact, and $V(C)$ acts via conjugation on H in the same way as does $\varphi(V(C))$. On the other hand we have the pushout along φ' :

$$\begin{array}{ccccccc} \mathfrak{E}_V: & 1 & \longrightarrow & V_H(G) & \longrightarrow & V(G) & \longrightarrow & V(C) & \longrightarrow & 1 \\ & & & \downarrow \varphi' & & \downarrow & & \parallel & & \\ {}_{\varphi'}\mathfrak{E}_V: & 1 & \longrightarrow & H & \longrightarrow & Y & \longrightarrow & V(C) & \longrightarrow & 1 \end{array}$$

In ${}_{\varphi'}\mathfrak{E}_V$ the group $V(C)$ acts on H via μ_I ; but since by construction $T \subset \text{Ker } \mu_I$, and since $\mu_I|_C = \mu$, $V(C)$ acts in the same way in both sequences ${}_{\varphi'}\mathfrak{E}_V$ and \mathfrak{E}_φ . But both sequences are split and so they are equivalent; i.e. we get a combined morphism

$$\begin{array}{ccccccc}
 1 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & C \longrightarrow 1 \\
 & & \uparrow \varphi' & & \uparrow \varphi & & \uparrow \varphi \\
 1 & \longrightarrow & V_H(G) & \longrightarrow & V(G) & \longrightarrow & V(C) \longrightarrow 1
 \end{array} \quad (D)$$

and hence we have constructed a splitting φ of the natural injection $G \rightarrow V(G)$. (We note that by [7], [12] $\text{Ker } \varphi$ is torsion free.) \square

We say that a splitting $\varphi: V(G) \rightarrow G$ comes from an ideal I , if φ renders the diagram (D) commutative and φ' is induced from a $\mathbb{Z}G$ -homomorphism $\eta \uparrow^G / I = H$ as above. In this case one must necessarily have $\text{Im } \mu_I \subset \text{Im } \mu$. Hence for a splitting φ to come from an ideal I is necessary and sufficient that $\text{Im } \mu_I \subset \text{Im } \mu$.

The Proposition 1 follows now immediately from Claim 2.

In order to get a workable condition, we return to the representation ν of (2).

Because of the isomorphism

$$\mathbb{Z}G\varepsilon_0 / \eta \uparrow^G \cong \eta \uparrow^G / \eta^2 \uparrow^G \cong \mathbb{F}_p C,$$

and because of Claim 1(iii), $\nu_i|_C$, $1 \leq i \leq m$, modulo \mathfrak{p} are the different irreducible representations in $\mathbb{F}_p C$. By Claim 1(iii), $\nu_i(c) / \nu_{i+1}^{-1}(c)$ modulo \mathfrak{p} is independent of i , say it is multiplication by α , a primitive m -th root of unity in \mathbb{F}_p . Thus, modulo \mathfrak{p} we have

$$\nu_i(c) = \nu_{i+1}(c)\alpha.$$

Since ν_i modulo \mathfrak{p} are the different irreducible representations, there exists an i_0 with

$$\nu_{i_0}(c) = \alpha \quad \text{modulo } \mathfrak{p}.$$

Hence after renumbering by passing to a sublattice of $M_0 = (R, \dots, R)^t$, on which G acts via $\mathbb{Z}G\varepsilon_0$, we may assume

$$\begin{aligned}
 &\nu_i \text{ modulo } \mathfrak{p} \text{ is induced from the representation} \\
 &c \mapsto \alpha^i, \quad 1 \leq i \leq n.
 \end{aligned} \quad (6)$$

If we denote by I_i the kernels of the map $\eta \uparrow^G \rightarrow \mathbb{F}_p^i$, $1 \leq i \leq m$, then these are two sided ideals, and so we can apply Claim 2.

Claim 3. *There exists a splitting of $G \rightarrow V(G)$ coming from an ideal I if and only if there exists an i , $1 \leq i \leq m$, such that*

$$\nu_i(u)\nu_{i+1}^{-1}(u)$$

modulo \mathfrak{p} has order dividing m for every $u \in V(C)$.

Proof of Claim 3. Let I be a two-sided ideal in $\eta \uparrow^G$ with $\eta \uparrow^G / I = H$, then by Claim 2, a splitting comes from an ideal I if and only if $\text{Im } \mu_I \subset \text{Im } \mu$; i.e. the elements in

$V(C)$ have to act on H with order dividing m , where the action is conjugation. Now, above we have found a decomposition of $\eta \uparrow^G / \eta^2 \uparrow^G$ as a direct sum of modules, on which $u \in V(C)$ acts as $v_i(u) v_{i+1}^{-1}(u)$, and hence by the Jordan–Hölder theorem, the action of u on $\eta \uparrow^G / I$ must be the same as the action of $v_i(u) / v_{i+1}^{-1}(u)$ on \mathbb{F}_p for some $1 \leq i \leq m$. \square

As an immediate consequence we obtain

Lemma 1. *If $m = p - 1$, then each of the ideals I_i , $1 \leq i \leq p - 1$, induces a splitting.*

Lemma 2. *If m is odd, then I_{i_0} gives a splitting for $i_0 = \frac{1}{2}(m - 1)$.*

Proof. We have a decomposition $V(C) = T \times C$, where T consists of real units, m being odd [8, Ch. III, §4, 4.1]. Hence if $*$: $\mathbb{Z}C \rightarrow \mathbb{Z}C$ is the involution induced by $c \mapsto c^{-1}$, then the elements in T are invariant under $*$. (This is proved in more generality in [3].) If now $u = \sum z_i c_i \in V(C)$, then by a proper choice of v_1 ,

$$v_{(m-1)/2}(u) = v_1 \left(\sum z_i c_i^{(m-1)/2} \right)$$

and

$$v_{(m-1)/2+1}(u) = v_1 \left(\sum z_i c_i^{(m-1)/2+1} \right),$$

i.e.

$$v_{(m-1)/2}(u) = v_{(m-1)/2+1}(u^*),$$

but for $u \in T$ we have $u = u^*$, and so

$$v_{(m-1)/2}(u) v_{(m-1)/2+1}^{-1}(u) = 1,$$

i.e. $I_{(m-1)/2}$ gives a splitting by Claim 3.

Remark. In general this is not the only splitting, as the following example shows: Let $G = C_{11} \rtimes C_5$, then $u = c + c^{-1} - 1$ is a unit in $\mathbb{Z}C_5$ which generates a complement in $V(C_5)$ to C_5 . If we put $\alpha = 4$ in \mathbb{F}_{11} and $v_i: c \mapsto \alpha^i$, then we have the following congruences modulo 11:

$$v_1(u) \equiv 6, \quad v_2(u) \equiv 2, \quad v_3(u) \equiv 2,$$

$$v_4(u) \equiv 6, \quad v_5(u) \equiv 1.$$

Hence for the quotients we have

$$v_1(u)/v_2^{-1}(u) \equiv 3, \quad v_2(u)/v_3^{-1}(u) \equiv 1, \quad v_3(u)/v_4^{-1}(u) \equiv 4,$$

$$v_4(u)/v_5^{-1}(u) \equiv 6, \quad v_5(u)/v_1^{-1}(u) \equiv 2.$$

Hence apart from the ideal I_2 (Lemma 2), also the ideals I_1 and I_3 yield splittings; but I_4 and I_5 can not be used to obtain splittings.

We now turn to our examples.

Example 1. Let $G = C_{73} \rtimes C_8$ and $C_8 = \langle c : c^8 = 1 \rangle$.

Claim 4. The element $u = 2 + c - c^3 - c^4 - c^5 + c^7$ is a unit in $\mathbb{Z}C_8$.

We first need:

Lemma 3. Let R be an integral domain with field of quotients K and $\Lambda \subset \Gamma$ R -orders in the finite dimensional K -algebra A . If $u \in \Lambda$ is a unit in Γ , then u is a unit in Λ .

Proof of Lemma 3. Let $\iota: \Lambda \rightarrow \Gamma$ be the inclusion, and denote by v_u the multiplication by u . Then we have the diagram

$$\begin{array}{ccccccc}
 & & & 0 & & & \\
 & & & \downarrow & & & \\
 0 & \longrightarrow & \Lambda & \xrightarrow{v_u} & \Lambda & \longrightarrow & \bar{\Lambda} \longrightarrow 0 \\
 & & \downarrow \iota & & \downarrow \iota & & \parallel \\
 0 & \longrightarrow & \Gamma & \xrightarrow{v_u} & \Gamma & \longrightarrow & 0 \longrightarrow 0
 \end{array}$$

Since Coker ι is artinian, v_u induces an automorphism on it and so $\bar{\Lambda} = 0$ by the 'snake' lemma. \square

Proof of Claim 4. Let

$$\Gamma = \mathbb{Z} \amalg \mathbb{Z} \amalg \mathbb{Z}[i] \amalg \mathbb{Z}[\zeta]$$

be the maximal order containing $\mathbb{Z}C_8$, where ζ is a primitive 8-th root of unity. Then the generator c of C_8 is represented as

$$c \mapsto (1, -1, i, \zeta),$$

and because of the above lemma, it suffices to show that u is a unit in Γ . We note that $1 + \zeta + \zeta^{-1}$ is a unit with inverse $(-1 + \zeta + \zeta^{-1})$ and

$$(1 + \zeta + \zeta^{-1})^2 = 2 + \zeta - \zeta^3 - \zeta^4 - \zeta^5 + \zeta^7.$$

Now since u is represented as

$$u \mapsto (1, 1, 1, 2 + \zeta - \zeta^3 - \zeta^4 - \zeta^5 + \zeta^7),$$

it is a unit in $\mathbb{Z}C_8$. \square

We now apply the above procedure: Since 10 is a primitive 8-th root of unity on \mathbb{F}_{73} , we have

$$v_1: c \mapsto 10,$$

for suitable choice of c and so an easy computation shows that

$$\begin{aligned} v_1(u) &\equiv -6 \pmod{73}, & v_2(u) &\equiv 1 \pmod{73}, \\ v_3(u) &\equiv 12 \pmod{73}, & v_4(u) &\equiv 1 \pmod{73}, \\ v_5(u) &\equiv 12 \pmod{73}, & v_6(u) &\equiv 1 \pmod{73}, \\ v_7(u) &\equiv -6 \pmod{73}, & v_8(u) &\equiv 1 \pmod{73}. \end{aligned}$$

Hence we obtain for the elements $v_i(u)v_{i+1}(u)^{-1}$ either 12 or $-6 \equiv 12^{-1}$ modulo 73. But both elements have order 36 modulo 73. Hence these calculations show, that for the group $G = C_{73} \wr C_8$ no ideal can yield a splitting.

Example 2. Let $G = C_{241} \wr C_{10}$ with $C_{10} = \langle c : c^{10} = 1 \rangle$. Then by the above remarks, $G_1 = C_{241} \wr C_2$ and $G_2 = C_{241} \wr C_5$ allow splittings which come from ideals, $\mathbb{Z}G_2$ has no non-trivial units. Hence it is necessary to construct a unit $u \in V(C_{10})$ which maps to the identity under $V(C_{10}) \rightarrow V(C_5) \times V(C_2)$.

Claim 5. *The element*

$$\begin{aligned} u = & -372099 c^0 + 114985 c^1 + 301035 c^2 - 301035 c^3 - 114985 c^4 \\ & + 372100 c^5 - 114985 c^6 - 301035 c^7 + 301035 c^8 + 114985 c^9 \end{aligned}$$

is a unit in $\mathbb{Z}C_{10}$ which maps to the identity under $V(C_{10}) \rightarrow V(C_5) \times V(C_2)$.

Proof. This can be proved by ‘brute force’; however, that does not show how we found u . Hence we take some space explaining it. The maximal order Γ containing $\mathbb{Z}C_{10}$ is

$$\Gamma = \mathbb{Z} \prod \mathbb{Z} \prod \mathbb{Z}[\zeta] \prod \mathbb{Z}[\zeta],$$

where ζ is a primitive 5-th root of unity. We choose the following embedding

$$\mathbb{Z}C_{10} \rightarrow \mathbb{Z} \prod \mathbb{Z} \prod \mathbb{Z}[\zeta] \prod \mathbb{Z}[\zeta], \quad c \mapsto (1, -1, \zeta, -\zeta).$$

If $\alpha: \mathbb{Z}C_{10} \rightarrow \mathbb{Z}C_2$ and $\beta: \mathbb{Z}C_{10} \rightarrow \mathbb{Z}C_5$ are the natural projections, then

$$\text{Ker } \alpha \cap \text{Ker } \beta \supset (0, 0, 0, 2(1 - \zeta)\mathbb{Z}[\zeta]),$$

and we have

$$(c^6 - 1)(c^5 - 1) = 1 + c - c^5 - c^6 = (0, 0, 0, 2(1 - \zeta)).$$

Now $u_0 = (\zeta^2 + \zeta^3 - 1)$ is a unit in $\mathbb{Z}[\zeta]$ with inverse $u_0^{-1} = (\zeta + \zeta^4 - 1)$. We are looking for a power u such that $u_0^n - 1 \in 2(1 - \zeta)\mathbb{Z}[\zeta]$. $n = 15$ will do, and

$$u_0^{15} = -514229 + 832040 \zeta^2 + 832040 \zeta^3$$

is congruent to 1 modulo $2(1 - \zeta)\mathbb{Z}[\zeta]$.

Observing

$$5 = (1 - \zeta)^4 \zeta^3 (1 - \zeta^2 - \zeta^3),$$

we can write u_0^{15} in the above form as an element in $\mathbb{Z}C_{10}$. \square

In order to apply Claim 3, there is no loss of generality if we assume (cf. (6))

$$v_1: c \mapsto 36 \quad \text{in } \mathbb{F}_{241}, \text{ modulo } p.$$

We put $v = c - c^5 + c^9$, then $v \in V(C_{10})$ with inverse $c^3 - c^5 + c^7$.

Assume now that for $G = C_{241} \wr C_{10}$ there would exist a splitting induced by an ideal. Then according to Claim 3, there exists an i , $1 \leq i \leq 10$, such that modulo p both

$$v_i(u)v_{i+1}^{-1}(u) \quad \text{and} \quad v_i(v)v_{i+1}^{-1}(v) \quad (7)$$

must have order in \mathbb{F}_{241} dividing 10. We put

$$\kappa_i = v_i(u)v_{i+1}^{-1}(u) \quad \text{and} \quad \lambda_i = v_i(v)v_{i+1}^{-1}(v).$$

Then by computation we obtain the list shown in Table 1.

Table 1

i	1	2	3	4	5	6	7	8	9	10
κ_i	233	233	30	1	1	233	30	30	233	30
λ_i	151	-1	83	191	53	151	-1	83	191	53

Hence u satisfies (7) only for $i = 4, 5$ and v satisfies (7) only for $i = 2, 7$. It should be noted that the above elements have the following order in \mathbb{F}_{241} :

$$|233| = |30| = 8 \quad \text{and} \quad 233^{-1} = 30,$$

$$|151| = |83| = 60 \quad \text{and} \quad 151^{-1} = 83,$$

$$|191| = |53| = 120 \quad \text{and} \quad 191^{-1} = 53.$$

Hence the table shows that for $G = C_{241} \wr C_{10}$ there can not exist a splitting induced by an ideal.

2. Congruence subgroup results

Again in this section $G = H \wr C$ is a Frobenius group $H = \langle h_0 : h_0^p = 1 \rangle$, for a prime $p \geq 7$ and $C = \langle c_0 : c_0^m = 1 \rangle$ with $2 < m \mid (p-1)$. The aim of this section is to show that if

$$\varphi: V(G) \rightarrow G$$

splits the natural inclusion, then it must essentially come from an ideal; i.e. the splittings described in the previous section are the only ones possible.

Proposition 2. *If $\varphi: V(G) \rightarrow G$ is a splitting as above, then φ renders the following diagram commutative:*

$$\begin{array}{ccccccc}
 1 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & C \longrightarrow 1 \\
 & & \uparrow \varphi' & & \uparrow \varphi & & \uparrow \varphi'' \\
 1 & \longrightarrow & V_H(G) & \longrightarrow & V(G) & \longrightarrow & V(C) \longrightarrow 1
 \end{array}$$

where $\varphi' = \varphi|_{V_H(G)}$ and $V_{\eta^2 \uparrow G}(G) \subset \text{Ker } \varphi'$.

The main tool in the proof is the use of Bass–Milnor–Serre’s congruence subgroup theorem [2], and we are indebted to H. Bass for pointing out that the kernel of φ' must contain a congruence subgroup.

The *proof* of the proposition will be done in several steps.

Claim 6. $\text{Im } \varphi|_{V_H(G)} = H$.

Proof. By [12], we can write

$$V_H(G) = T_1 \downarrow H \quad (8)$$

as a semidirect product with $T_1 = V_{\eta^2 \uparrow G}(G)$ a torsion-free group. We consider $\varphi' = \varphi|_{V_H(G)}$. Since $V(G)/V_H(G)$ is abelian, $\text{Im } \varphi' \supset H$, and so $\text{Im } \varphi' = H \downarrow \tilde{C}$ for a subgroup \tilde{C} of C . Moreover, $\varphi'(1 + (h-1)) = h$ since φ is a splitting and $H \leq V_H(G)$. Thus $(\varphi')^{-1}(H) \supset H$ and so

$$(\varphi')^{-1}(H) = T_2 \downarrow H.$$

But then

$$T_1/T_2 \downarrow H \cong H \downarrow \tilde{C};$$

however, such an isomorphism can only exist if $\tilde{C} = 1$, since in one group H is a complement, in the other group, H is a Frobenius kernel. \square

We note that by means of Claim 6, the above diagram is commutative, and it remains to show $V_{\eta^2 \uparrow G}(G) \subset \text{Ker } \varphi'$.

We now have to introduce some more *notations*: If $\mathfrak{a} \neq 0$ is an ideal in R (cf. (2)), we denote by $\Gamma_m(\mathfrak{a})$ the congruence subgroup in $\text{SL}_m(R)$ with respect to \mathfrak{a} ; i.e. the kernel of the natural map

$$\text{SL}_m(R) \rightarrow \text{SL}_m(R/\mathfrak{a}).$$

We denote by e_{ij} the $m \times m$ matrix with 1 at the (i, j) -position and 0 elsewhere. $E_m(\mathfrak{a})$ is the normal subgroup of $\text{SL}_m(R)$ generated by the \mathfrak{a} -elementary matrices $E + \alpha e_{ij}$, $\alpha \in \mathfrak{a}$, $i \neq j$, where E denotes the $m \times m$ identity matrix.

For an ideal $I \subset \eta \uparrow^G$ we put

$$\begin{aligned} \mathrm{SV}_I(G) &= \{u \in V_I(G) : \det u = 1\} \\ &= V_I(G) \cap \mathrm{SL}_m(R) \quad (\text{cf. (3)}). \end{aligned} \quad (9)$$

If R_1^* are the units in R congruent to 1 modulo \mathfrak{p} , then

$$R_1^* = \tilde{R}_1^* = \left\{ \begin{bmatrix} 1+x & & \\ & 1 & \\ & & \ddots \\ & & & 1 \end{bmatrix}_m, x \in \mathfrak{p} \right\} \cap \mathrm{GL}_m(R) \quad (10)$$

is a subgroup of $V_H(G)$ (cf. (3)), and

$$V_H(G) = \mathrm{SV}_H(G) \tilde{R}_1^*.$$

Since $m \neq 1$, the only roots of unity in R are ± 1 , and so the elements in $H_1 < V_H(G)$ (cf. (8)) lie in $\mathrm{SV}_H(G)$; i.e.

$$\varphi' |_{\mathrm{SV}_H(G)} : \mathrm{SV}_H(G) \rightarrow H$$

is surjective. We put

$$\varphi'_S = \varphi' |_{\mathrm{SV}_H(G)}. \quad (11)$$

Claim 7. $\mathrm{Ker} \varphi'_S$ contains the congruence subgroup $\Gamma_m(\mathfrak{p}^2)$.

Proof. Using the relation

$$[1 + \alpha e_{ik}, 1 + \beta e_{kj}] = 1 + \alpha \beta e_{ij}$$

for i, j, k distinct, note $m > 2$, and we obtain – observing that H is abelian – that the subgroup

W of $\mathrm{SL}_m(R)$ generated by

$$\begin{aligned} &\{1 + re_{ij} : j - i \geq 2, r \in R\} \\ &\cup \{1 + \alpha e_{r,s}, r \neq s, -(m-2) \leq s - r \leq 1, \alpha \in \mathfrak{p}\} \\ &\cup \{1 + \beta e_{m,1}, \beta \in \mathfrak{p}^2\} \end{aligned} \quad (12)$$

lies in the kernel of φ'_S .

In particular, $E_m(\mathfrak{p}^2) \subset \mathrm{Ker} \varphi'_S =: N$. Now, since the only units of finite order in R are ± 1 , we conclude with [2, 3.6]

$$|\Gamma_m(\mathfrak{p}^2) : E_m(\mathfrak{p}^2)| \leq 2.$$

On the other hand, $\mathrm{SV}_H(G) \supset \Gamma_m(\mathfrak{p})$ and since $|\mathrm{SV}_H(G) : N|$ is odd, we have

$$\Gamma_m(\mathfrak{p}^2) \subset N,$$

as claimed. \square

The remaining part of the *proof of Proposition 2* concerns only questions about some very common finite groups.

Claim 8. $SV_{n^2 \uparrow G}(G) \subset \text{Ker } \varphi'_S =: N$.

Proof. By Claim 7 and the fact that $SL_m(R) \rightarrow SL_m(R/p^2)$ is surjective (both groups are generated by elementary matrices) we are reduced to a question about subgroups of $SL_m(R/p^2)$.

We view the latter as an extension

$$0 \rightarrow M \rightarrow SL_m(R/p^2) \rightarrow SL_m(R/p) \rightarrow 1,$$

where $M = \mathfrak{sl}_m(R/p)$ is the module consisting of $m \times m$ matrices of trace zero. The corresponding sequence of the image of $SV_H(G)$ in $SL_m(R/p^2)$, denoted by $\overline{SV_H(G)}$, is

$$0 \rightarrow M \rightarrow \overline{SV_H(G)} \rightarrow U \rightarrow 1,$$

where

$$U = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}_{m \times n}$$

is the unipotent radical of the standard Borel subgroup of $SL_m(p)$. Let M' be the submodule of M consisting of the matrices with zero in the lower left hand corner $((m, 1)$ -position), and put M'' to be the submodule of M' consisting of the matrices of M' with zero diagonal entries. Then the subgroup W defined in (12) has image in $SL_m(R/p^2)$ containing M'' . Since the conjugate of $e_{i,i+1}$ under $1 + e_{i+1,i}$ is

$$e_{i,i+1} + e_{i+1,i+1} - e_{ii} - e_{i+1,i},$$

the W -submodule of M' generated by M'' contains the generators $e_{i+1,i+1} - e_{ii}$ of the trace zero matrices, and thus all of M' . Since W contains $1 + Re_{ij}$ for $j - i \geq 2$ and because of the structure of $n^2 \uparrow G$ (cf. (3)), the claim follows easily. \square

Claim 9. $\text{Ker } \varphi' = \text{Ker } \varphi|_{V_H(G)}$ contains $V_{n^2 \uparrow G}(G)$.

Proof. We note from (3), that $V_{n^2 \uparrow G}(G)$ contains \tilde{R}_1^* (cf. (10)), hence

$$V_{n^2 \uparrow G}(G) = SV_{n^2 \uparrow G}(G)\tilde{R}_1^*.$$

We have the commutative diagram

$$\begin{array}{ccccccc} & & D & \xrightarrow{\sim} & \tilde{R}_1^* & & \\ & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & \text{Ker } \varphi' & \longrightarrow & V_H(G) & \xrightarrow{\varphi'} & H \longrightarrow 1 \\ & & \uparrow & & \uparrow & & \parallel \\ 1 & \longrightarrow & \text{Ker } \varphi'_S & \longrightarrow & SV_H(G) & \xrightarrow{\varphi'_S} & H \longrightarrow 1 \end{array}$$

Hence $D = \tilde{R}_1^*$ and $\text{Ker } \varphi' = \text{Ker } \varphi'_5 D$.

We note that $\tilde{R}_1^* \subset \text{Ker } \varphi' (10)$. To see this, observe first that

$$\varphi(\tilde{R}_1^*) = \varphi(\tilde{R}_1^* \Gamma_m(\mathfrak{p}^2) / \Gamma_m(\mathfrak{p}^2))$$

has order 1 or p , in the latter case we have $\varphi(\tilde{R}_1^*) = H$. However, $\tilde{R}_1^* \Gamma_m(\mathfrak{p}^2) / \Gamma_m(\mathfrak{p}^2)$ is clearly centralized by the group C which is represented diagonally in $\mathbb{Z}G_0 / \Gamma_m(\mathfrak{p})$. So we must have that $\varphi(\tilde{R}_1^*)$ commutes with $\varphi(C) = C$. This gives $\varphi(\tilde{R}_1^*) = 1$. Now it follows

$$V_{\eta^2 \uparrow G}(G) = SV_{\eta^2 \uparrow G}(G) \tilde{R}_1^* \subset \text{Ker } \varphi'$$

by Claim 8.

This also proves Proposition 2. \square

We now are finally in the position to prove that our splitting φ comes 'essentially' from an ideal.

From the proposition it follows that we obtain a $V(C)$ -homomorphism – note that $V_H(G) / V_{\eta^2 \uparrow G}(G)$ is abelian:

$$\bar{\varphi}: V_H(G) / V_{\eta^2 \uparrow G}(G) \rightarrow H.$$

Combining this with the $V(C)$ -isomorphism from Claim 1(i)

$$V_H(G) / V_{\eta^2 \uparrow G}(G) \cong \eta \uparrow^G / \eta^2 \uparrow^G,$$

we conclude that the $V(C)$ -action on H induced from φ must be the same as the $V(C)$ -action on H induced by one of the ideals I_j , $1 \leq j \leq m$ (Claim 3), and so there must also exist a splitting induced by I_j for some $1 \leq j \leq m$, such that both $V(C)$ -actions are the same. Applying this to our examples we conclude:

Proposition 3. *For the Frobenius groups $C_{73} \wr C_8$ and $C_{241} \wr C_{10}$ there can not exist a homomorphism $\varphi: V(G) \rightarrow G$ splitting the natural injection $G \rightarrow V(G)$.*

References

- [1] P.J. Allan and C. Hobby, A characterization of units in $\mathbb{Z}[A_4]$, Abstracts AMS 1, 773-20-10 (1980).
- [2] H. Bass, J. Milnor and J.P. Serre, Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$), Publ. I.H.E.S. No. 33 (1967).
- [3] G.H. Cliff, S.K. Sehgal and A.R. Weiss, Units of integral grouprings of metabelian groups, J. Algebra 73 (1981) 167–185.
- [4] K. Dennis, The structure of the unit group of group rings, Proceedings of the Ring Theory Conference, Oklahoma 1976 (Marcel Dekker).
- [5] S. Galovich, I. Reiner and S. Ullom, Class groups for integral representations of metacyclic groups, Matematika 19 (1972) 105–111.
- [6] G. Higman, Units in group rings, Ph.D. Thesis, Balliol College, Oxford (1940).
- [7] D.A. Jackson, The groups of units of the integral group rings of finite metabelian and finite nilpotent groups, Quart. J. Math. Oxford 20 (2) (1969) 319–331.

- [8] S. Lang, *Cyclotomic Fields*, Graduate Texts in Math. (Springer, Berlin–New York, 1978).
- [9] T. Miyata, On the units of the integral group ring of a dihedral group, *J. Math. Soc. Japan* 32 (1980) 703–708.
- [10] D. Passman and P.F. Smith, Units in integral group rings, *J. Algebra* 69 (1981) 213–239.
- [11] K.W. Roggenkamp, Zur Einheitengruppe der ganzzahligen Gruppenringe metazyklischer Frobeniusgruppen, *Arch. Math.* 35 (3) (1980) 263–266.
- [12] K.W. Roggenkamp, Units in integral metabelian group rings I, Jackson's unit theorem revisited, *Quart. J. Math. Oxford* 32 (126) (1981) 209–224.
- [13] K.W. Roggenkamp, *Representation Theory of Finite Groups*, 18^e Session Séminaire de Mathématiques Supérieures (Presses de l'Université de Montréal, 1980) 1–165.
- [14] K. Sekiguchi, Letter to K.W. Roggenkamp from Nov. 4, 1980.